

EXHIBIT B

COPY

File No.		STATE OF NORTH CAROLINA		In The General Court Of Justice District/Superior Court Division	
SEARCH WARRANT		Rockingham		County	
IN THE MATTER OF					
Roberta Hill and Brian Hill					
Date Issued	8/28/12	Time Issued	11:30	<input checked="" type="checkbox"/> AM	<input type="checkbox"/> PM
Name Of Applicant	Todd Britton				
Name Of Additional Affiant	Robert Bridge				
Name Of Additional Affiant	Hobbes				
RETURN OF SERVICE					
I certify that this Search Warrant was received and executed as follows:					
Date Received		Time Received		<input type="checkbox"/> AM	<input type="checkbox"/> PM
Date Executed		Time Executed		<input type="checkbox"/> AM	<input type="checkbox"/> PM
<input type="checkbox"/> I made a search of _____					
_____ as commanded.					
<input type="checkbox"/> I seized the items listed on the attached inventory.					
<input type="checkbox"/> I did not seize any items.					
<input type="checkbox"/> This Warrant WAS NOT executed within forty-eight (48) hours of the date of issuance and I hereby return it not executed.					
Name Of Officer Making Return (Type Or Print)		Time	<input type="checkbox"/> AM	<input type="checkbox"/> PM	Signature Of Magistrate
Signature Of Officer Making Return					
This Search Warrant was returned to the undersigned clerk on the date and time shown below.					
Date		Time	<input type="checkbox"/> AM	<input type="checkbox"/> PM	Signature Of Clerk
Department Or Agency Of Officer					
Incident Number					
Dep CSC <input type="checkbox"/> Asst CSC <input type="checkbox"/> CSC <input type="checkbox"/>					

APPLICATION FOR SEARCH WARRANT

I, Sergeant Todd Brim, Mayodan Police Department

(Insert name and address; or if law enforcement officer, name, rank and agency)

being duly sworn, request that the Court issue a warrant to search the person, place, vehicle, and other items described in this application and to find and seize the property and person described in this application. There is probable cause to believe that (Describe property to be seized; or if search warrant is to be used for searching a place to serve an arrest warrant or other process, name person to be arrested)

Attachment A

constitutes evidence of a crime and the identity of a person participating in a crime, (Name crime) Second Degree Sexual Exploitation of a Minor

and is located (Check appropriate box(es) and fill-in specified information)

☒ in the following premises (Give address and, if useful, describe premises)

Attachment B

(and)

☒ on the following person(s) (Give name(s) and, if useful, describe person(s))

Attachment B

(and)

☒ in the following vehicle(s) (Describe vehicle(s))

Attachment B

(and)

☐ (Name and/or describe other places or items to be searched, if applicable)

The applicant swears or affirms to the following facts to establish probable cause for the issuance of a search warrant:

Attachment C and Attachment D

SWORN/AFFIRMED AND SUBSCRIBED TO BEFORE ME

Date
8/28/12

Name Of Applicant (Type Or Print)
Todd Brim Robert B. B.

Signature
[Signature]

Signature Of Applicant
[Signature]

☐ Magistrate

☐ Dep. CSC

☐ Asst. CSC

☐ Clerk Of Superior Court

☒ Judge

☐ In addition to the affidavit included above, this application is supported by additional affidavits, attached, made by Det. Robert Bridge, Reidsville Police Department

☐ In addition to the affidavit included above, this application is supported by sworn testimony, given by

This testimony has been (check appropriate box) ☐ reduced to writing

☐ tape recorded and I have filed each with the clerk.

NOTE: If more space is needed for any section, continue the statement on an attached sheet of paper with a notation saying "see attachment." Date the continuation and include on it the signatures of applicant and issuing official.

ATTACHMENT A

ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense; or contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely a violation of NCGS 14-190.17:

1. Computers and computer related storage media including, but not limited to, hard drives, thumb drives, CDs, DVDs, floppy disks, flash media, memory sticks, iPods, PDAs (Personal Digital Assistant), cell phones and any other mobile wireless devices, and other magnetic, digital, and/or optical recording media.
2. Records evidencing use or moderation of a Gnutella P2P network including, but not limited to, screen names, filenames, digital pictures, dates/times of posted images,
3. IP connection information related to the postings.
4. Graphic and movie files (including, but not limited to, files bearing file extensions .JPG, .GIF, .TIF, .AVI, .MPG, and WMV,), and the data within the aforesaid objects relating to said materials, which may be, or are, used to visually depict child pornography or child erotica.
5. Computer programs capable of viewing graphic files.
6. Text files containing information pertaining to the interest in child pornography or sexual activity with children and/or pertaining to the production, trafficking in, or possession of child pornography.
7. Correspondence, including, but not limited to, electronic mail, chat logs, and electronic messages, pertaining to the trafficking in, production of, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in NCGS 14-190.17.
8. Correspondence including, but not limited to electronic mail, chat logs, electronic messages, soliciting minors to engage in sexually explicit conduct for the purposes of committing an unlawful sex act and/or producing child pornography.
9. Any child pornography in any form including, but not limited to, photographs, magazines, photocopies of photographs, videocassette tapes, and computer text or images.
10. Names and addresses of minors visually depicted while engaged in sexually explicit conduct.
11. Files depicting sexual conduct, whether between adults or between adults and minors.
12. Any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography.
13. Any and all documents and records pertaining to the purchase of color photographs or the purchase of any child pornography.
14. Notations of any password that may control access to a computer operating system or individual computer files. Evidence of payment for child pornography, including but not limited to: cancelled checks, money order receipts, or a debit entry in a computer software finance program or credit card statement.
15. Computers, keyboards, tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disks drives, monitors, computer printers, modems, tape drives, disk applications programs, data disks, system disk operating systems, magnetic media floppy disks, Secure Digital Disks, USB Drives, digital cameras, hardware and software operating manuals, tape systems and hard drive.

Signature: Judicial Official/Date

Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

Additional Affiant: Signature/Date

Todd Brim, Detective Sergeant

Mayodan Police Department

T Brim

Sworn to and subscribed before

Me this, the 28 day of August, 2012

J. Todd Brim

Judicial Official

J. Todd Brim 8/28/12

Signature: Judicial Official/Date

T Brim 8/28/12

Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

None 8/28/12

2

ATTACHMENT B

DESCRIPTION OF PLACES TO BE SEARCHED

The residence, persons and vehicles located on the premises of 413 North 2nd Avenue, in Mayodan, North Carolina. The home, person, and vehicles of Roberta Hill W/F DOB: 05/14/1967 NC OLN: 8867196 and Brian David Hill W/M DOB: 5/26/1990 NC OLN: 38360908 and/or any other person at the residence of at 413 N 2nd Ave. to include any vehicles located at that address: specifically registered to Roberta Hill and that are associated with the home specifically a 2000 Pontiac Sunfire Plate# PWA6942.

The residence can be reached leaving the Mayodan Police Department:

1. Start out going southwest on N 3rd Ave toward W Main St. 0.01 mi

Zoom to this Step Main St. 0.07 mi

Force Left Turn the left?
If you are on E Main St and reach W Main St you've gone a little too far.

3. Take the 1st left onto N 2nd Ave/US-220-BR. 0.4 mi

Star Photo is on the left
If you are on E Main St and reach W Main Ave you've gone a little too far.

4. 413 N 2ND AVE is on the right.

Your destination is just past W Van Buren St.
If you reach N 1st Ave you've gone a little too far.

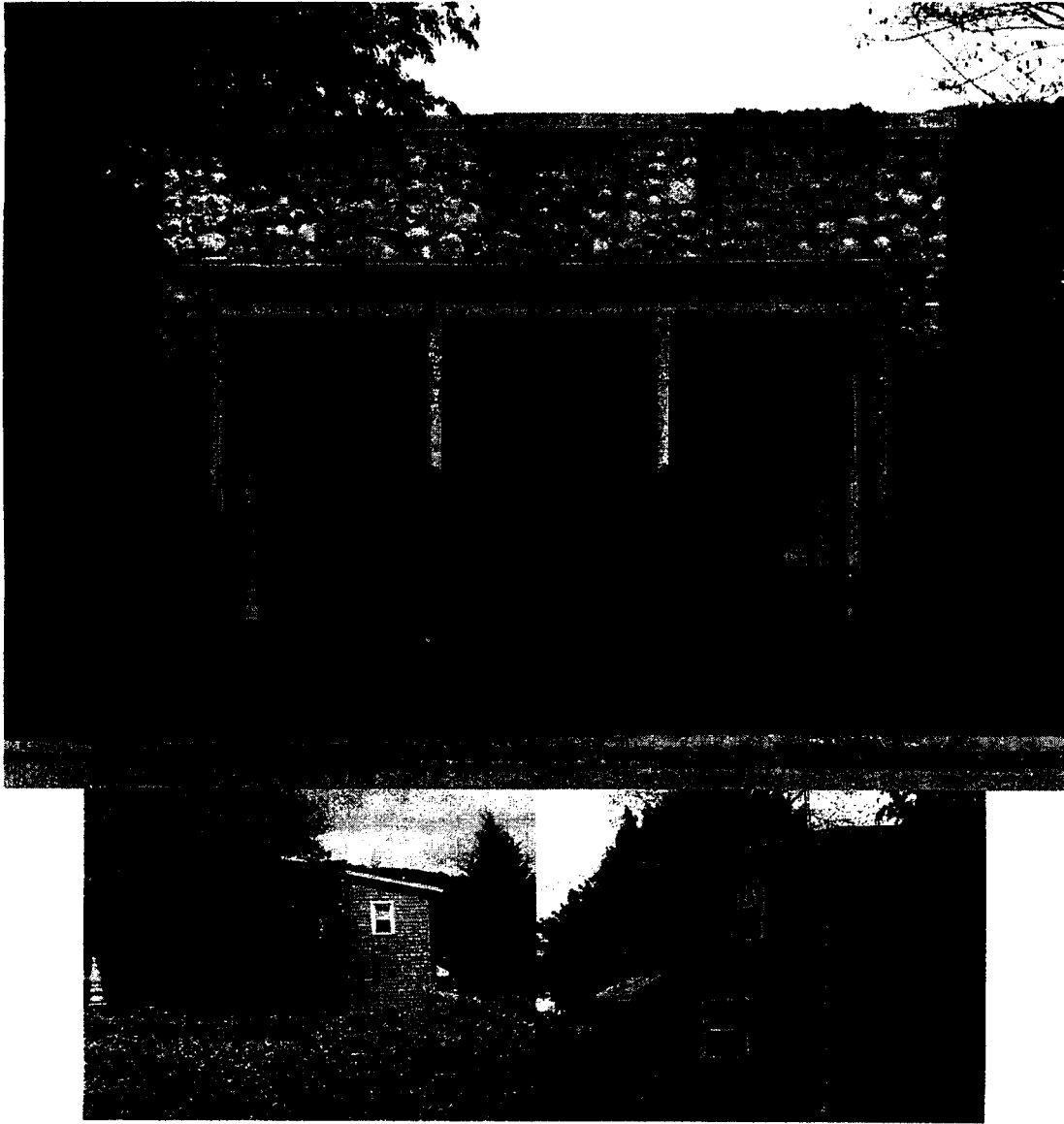


2. 2nd Ave 8/28/12
Signature: Judicial Official/Date

GTBun 8/28/12
Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

8/28/12
Additional Affiant: Signature/Date



J. J. H. 8/28/12
 Signature: Judicial Official/Date

 Additional Affiant: Signature/Date

G. B. 8/28/12
 Signature: Law Enforcement/Date

W. 8/28/12
 Additional Affiant: Signature/Date

Attachment C

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Todd Brim, (YOUR AFFIANT) being duly sworn, do hereby depose and say:

BACKGROUND ON AFFIANT: Todd Brim, Mayodan Police Detective Sergeant employment, educational and training background is as follows:

1. I (YOUR AFFIANT) received my Basic Law Enforcement Training Certificate (BLET) in 1995. While in BLET, I received the highest grade point average in my class. I was hired as a Police Officer for the Town of Mayodan, NC in 1995. I was assigned as a patrol officer, where I conducted investigations into automobile accidents, misdemeanor larcenies, and minor drug possessions. In 1998, your affiant was promoted to the Criminal Investigations unit as a Criminal Detective. Your affiant has taken several courses from the North Carolina Justice Academy including Interview and Interrogation, Police Law Institute, and Basic Cyber Crimes Investigations. I have successfully completed the North Carolina Justice Academy's Criminal Investigation Certificate Program and I have obtained my Advanced Law Enforcement Certificate.
2. I, Todd Brim, have previously written affidavits for search warrants in cases involving various crimes committed in the Town.
3. This affidavit is made in support of an affidavit for a search warrant to search the premises and computer equipment of the residence (413 N 2nd Ave, Mayodan, North Carolina,), person, and vehicles of Roberta Hill W/F DOB: 05/14/1967 NC OLN: 8867196 and Brian David Hill W/M DOB: 5/26/1990 NC OLN: 38360908 and/or any other person at the residence of at 413 N 2nd Ave. to include any vehicles located at that address: specifically registered to Roberta Hill and that are associated with the home specifically a 2000 Pontiac Sunfire Plate# PWA6942. Records indicate that Roberta Hill is the occupant and Brian David Hill is known by police officers to live at this residence. Records also indicate that Roberta Hill has a subscription and service for Time Warner Cable Internet Service at that address that matches the IP addresses where child pornography has been captured during this investigation.

OVERVIEW OF PROBABLE CAUSE

4. The information contained within this affidavit is based upon information your affiant has gained from my investigation, personal observations, training and experience, and/or information related to your affiant by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of assisting in securing a search warrant, your affiant has not included each and every fact known to me concerning this investigation. Your affiant has set forth the facts believed to be necessary to establish probable cause to believe that evidence of violations of North Carolina G.S. 14-190.17, second degree sexual exploitation of a minor, will be found on the premises, and on the computers and/or electronic storage media located on the premises.

2. Todd Brim 8/28/12
Signature: Judicial Official/Date

T Brim 8/28/12
Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

Reddy 8/28/12
Additional Affiant: Signature/Date

5. On Wednesday, August 22, 2012 at 1400 hours, Reidsville Police Detective Robert Bridge contacted me in reference to a child pornography case in the Town of Mayodan, North Carolina. According to Detective Bridge, he discovered that an IP address registered to Roberta Hill was being used to download and view child pornography. Detective Bridge is a member of the Internet Crimes Against Children (ICAC) Task Force. He has received training and resources to successfully investigate cybercrimes involving child pornography.
6. Detective Bridge requested that I confirm that no other "Wi-Fi" signals were in the area of the Hill residence, located at 413 North 2nd Avenue in Mayodan, North Carolina. Furthermore, he requested that we confirm any known occupants of the residence. Through my knowledge and previous experience, I know the residence is occupied by Roberta Hill and her son, Brian D. Hill. I drove to the residence and confirmed that no unsecured "Wi-Fi" signals were present at the time of this affidavit. I also checked the utilities and confirmed that Roberta Hill resides and the aforementioned address.

2. [Signature] 8/28/12
Signature: Judicial Official/Date

Additional Affiant: Signature/Date

G. T. Bunn 8/28/12
Signature: Law Enforcement/Date

[Signature] 8/28/12
Additional Affiant: Signature/Date

Attachment D

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT


I, Robert W Bridge, (YOUR AFFIANT) being duly sworn, do hereby depose and say:

BACKGROUND ON AFFIANT: Robert W Bridge, Reidsville Police Detective employment, educational and training background is as follows:

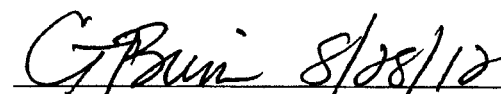
7. I (YOUR AFFIANT) Received my Basic Law Enforcement Training Certificate (BLET) in 2008. While in BLET I received the highest grade point average in my class. I graduated from Rockingham Community College with honors with an Associate in Applied Science in Criminal Justice Technology. I am currently attending Guilford College studying Computer Technology Information Systems. I was hired as a Police Officer for the City Of Reidsville, NC in 2009. I was assigned as a patrol officer where I conducted investigations into automobile accidents misdemeanor larcenies, and minor drug possessions. In 2011 your affiant was promoted to the Criminal Investigations unit as the Juvenile Detective. I also was given a position on the North Carolina Internet Crimes against Children task force. As part of that task force your affiant has completed 110 hours of training in internet related investigations including basic undercover internet investigations, peer to peer file sharing undercover investigations, wireless network investigations, craigslist investigations and computer triages. Your affiant has also taken several courses from the North Carolina Justice Academy including Interview and Interrogation, Police Law Institute, and Child about Related Interviewing: The Suspected Predator.
8. I, Robert Bridge, have previously written affidavits for search warrants in cases involving crimes against children, child exploitation, Internet crimes against children and cases arising out of various on-line undercover in crimes against children, as well as all other facets of criminal investigations.
9. This affidavit is made in support of an affidavit for a search warrant to search the premises and computer equipment of the residence (413 N 2nd Ave, Mayodan, North Carolina,), person, and vehicles of Roberta Hill W/F DOB: 05/14/1967 NC OLN: 8867196 and Brian David Hill W/M DOB: 5/26/1990 NC OLN: 38360908 and/or any other person at the residence of at 413 N 2nd Ave. to include any vehicles located at that address: specifically registered to Roberta Hill and that are associated with the home specifically a 2000 Pontiac Sunfire Plate# PWA6942. Records indicate that Roberta Hill is the occupant and Brian David Hill is known by police officers to live at this residence. Records also indicate that Roberta Hill has a subscription and service for Time Warner Cable Internet Service at that address that matches the IP addresses where child pornography has been captured during this investigation.

OVERVIEW OF PROBABLE CAUSE

10. The information contained within this affidavit is based upon information your affiant has gained from my investigation, personal observations, training and experience, and/or information related to your affiant by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of assisting in securing a search warrant, your affiant has not


Signature: Judicial Official/Date

Additional Affiant: Signature/Date


Signature: Law Enforcement/Date


Additional Affiant: Signature/Date

included each and every fact known to me concerning this investigation. Your affiant has set forth the facts believed to be necessary to establish probable cause to believe that evidence of violations of North Carolina G.S. 14-190.17, second degree sexual exploitation of a minor, will be found on the premises, and on the computers and/or electronic storage media located on the premises. Specifically this affidavit will show the scope and nature of how the IP addresses (24.148.156.211) assigned to 413 2nd Ave, Mayodan NC, the home of of Roberta Hill W/F DOB: 05/14/1967 NC OLN: 8867196 and Brian David Hill W/M DOB: 5/26/1990 NC OLN: 38360908, was located and identified in an ongoing undercover investigation into child pornography trading on the Internet. It will show how automated tools used in that undercover process recorded the IP address sharing child pornography and how automated undercover tools were used to get a list of files on the computer at that IP address and to download some of the offered child pornography. It will show how that child pornography is known to be illegal in North Carolina. It will describe the scope and breadth of the undercover operation and how it relates specifically to this IP address and address. It will show that I made a direct connection to the computer at that IP address and received a listing of files and digital signatures of those files on the computer at the IP address. It will show that your affiant downloaded files of child pornography over a period of time from that IP address. It will show what your affiant knows about each of the files that were on, and are expected to be found on the computer at the IP addresses (24.148.156.211).

BACKGROUND ON OFFENSES AND STATUTORY AUTHORITY

11. NCGS 14-190.17, known as Second Degree Sexual Exploitation of a Minor makes it unlawful for a person if, knowing the character or content of the material he distributes, transports, exhibits, receives, sells, purchases, exchanges, or solicits material that contains a visual representation of a minor engaged in sexual activity.
12. NCGS 14-190.13, known as Definitions for Certain Offenses Concerning Minors provides the following definitions as applied to NCGS 14-190.14, Displaying Material Harmful to Minors; NCGS 14-190.15, Disseminating or Exhibiting to Minors Harmful Material or Performances; NCGS 14-190.16, First Degree Sexual Exploitation of a Minor; NCGS 14-190.17, Second Degree Sexual Exploitation of a Minor; NCGS 14-190.17A, Third Degree Sexual Exploitation of A Minor; NCGS 14-190.18, Promoting Prostitution of a Minor; and NCGS 14-190.19, Participating in Prostitution of a Minor.

- Harmful to Minors. - That quality of any material or performance that depicts sexually explicit nudity or sexual activity and that, taken as a whole, has the following characteristics: The average adult person applying contemporary community standards would find that the material or performance has a predominant tendency to appeal to a prurient interest of minors in sex; and The average adult person applying contemporary community standards would find that the depiction of sexually explicit nudity or sexual activity in the material or performance is patently offensive to prevailing standards in the adult community concerning what is suitable for minors; and
- The material or performance lacks serious literary, artistic, political, or scientific value for minors.
- Material. - Pictures, drawings, video recordings, films or other visual depictions or representations but not material consisting entirely of written words.
- Minor. - An individual who is less than 18 years old and is not married or judicially

J. L. Hill 8/28/12
Signature: Judicial Official/Date

CTBum 8/28/12
Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

8/28/12
Additional Affiant: Signature/Date

emancipated.

- Prostitution. - Engaging or offering to engage in sexual activity with or for another in exchange for anything of value.
- Sexual Activity. - Any of the following acts:
 - Masturbation, whether done alone or with another human or an animal.
 - Vaginal, anal, or oral intercourse, whether done with another human or with an animal.
 - Touching, in an act of apparent sexual stimulation or sexual abuse, of the clothed or unclothed genitals, pubic area, or buttocks of another person or the clothed or unclothed breasts of a human female.
 - An act or condition that depicts torture, physical restraint by being fettered or bound, or flagellation of or by a person clad in undergarments or in revealing or bizarre costume.
 - Excretory functions; provided, however, that this sub-subdivision shall not apply to G.S. 14-190.17A.
 - The insertion of any part of a person's body, other than the male sexual organ, or of any object into another person's anus or vagina, except when done as part of a recognized medical procedure.
 - The lascivious exhibition of the genitals or pubic area of any person.
 - Sexually Explicit Nudity. - The showing of: Uncovered, or less than opaquely covered, human genitals, pubic area, or buttocks, or the nipple or any portion of the areola of the human female breast, except as provided in G.S. 14-190.9(b); or
 - Covered human male genitals in a discernibly turgid state.

BACKGROUND ON MAINTAINING CONTRABAND AND STALENESS ISSUES

13. Through your affiant's training and experience working cases involving child pornography and through consulting with others experts in the field your affiant has learned and believes that Illegal contraband such as Child Pornography and other materials like Child Erotica and Incest literature is typically collected, stored and distributed by individuals that trade in this type of illegal activity. This type of contraband (Collected Child Pornography) is not "used up" as other Types of contraband can be such as alcohol or drugs. This type of evidence is usually stored in a manner that is easily accessible to the subject viewing these images and is usually stored on a computer's hard drive or some other type of accessible electronic storage media, and may be stored off-site via the use of an Internet Service Provider (ISP). Additionally, email and other data files can typically be stored online, and is usually only limited by the amount of storage space used by the account holder. A small 1 inch square object such as a Secure Digital Storage card can literally hold up to thousands of images. For these reasons contraband of this type can and is usually stored for indefinite amounts of time by the possessors of this illegal contraband. In your affiant's experience and training, and through consultation with other experts, it is known that in many instances these types of files have been found that were stored for years and transferred from and between storage medium and from computer to computer where new computers are obtained by those who collect and trade in child pornography.
14. Collections of child pornography vary in size and in the items based on many factors. Factors which can determine the size and extent of a collection include: living arrangements, economic status, and age. Older offenders and offenders with living arrangements that allow for privacy

2 Julie E. G. 8/28/12
Signature: Judicial Official/Date

G. Bruni 8/28/12
Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

ADW 8/28/12
Additional Affiant: Signature/Date


tend to have larger collections.


15. The use of the computer has changed some of these behaviors. Computers allow for an individual to collect items and more easily hide their collection from others. The computer has in essence, allowed the individual who views or collects child pornography to maintain a certain anonymity via the Internet through the use of aliases known as "screen names" or "user names," as well as allowing for the storage of the collection and easy retrieval for viewing. The computer has also made it easy for individuals with similar behaviors to contact, exchange information and validate their behavior amongst each other.

Through the training and experience of this Detective and others listed in this affidavit, I know that individuals who view and or collect child pornography, even if viewing these items from an off-site location, generally maintain the ability to view and store these types of items in their residence or a secure and easily accessible place, especially through the use of a computer and or digital devices for long periods of time. Since child pornography materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time. Computers and other digital media are akin to a filing cabinet or a vault. More germane to this investigation, images and videos of child pornography are hoarded by those who possess it. People who possess these images, rarely, if ever, dispose of it as the sexually explicit material is treated as a prize possession. It acts as a sexual stimulus and provides sexual gratification. Great lengths will be taken to conceal and protect from discovery, theft, and damage their collections of illicit materials. The images and videos of child pornography may be moved around to different parts of the computer or moved to different external media, but it is maintained as a collection for months and years.

SEARCH AND SEIZURE OF COMPUTERS AND RELATED MEDIA

16. Based upon your affiant's training and experience and consultations with other law enforcement officers who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching and seizing information from computers often requires law enforcement officers to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. That process is lengthy and time consuming and takes days and even weeks. This is true because computer storage devices (like hard disks, diskettes, tapes, laser disks, CD-ROMs) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. While an on-site computer preview is beneficial to get an initial glimpse of some of the items stored on the media, searching authorities will be required to examine all the stored data to determine which particular files are evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of full data search on site. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize

 8/28/12
Signature: Judicial Official/Date

 8/28/12
Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

 8/28/12
Additional Affiant: Signature/Date 10

in some systems and applications, so it is often times difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis. Therefore removal from the premises of some or all computer equipment and related storage media will be required for proper analysis and specific permission by this search and seizure warrant to remove the computer equipment and search it over time at a later date is sought.

BACKGROUND ON PEER-TO-PEER NETWORKS AND THIS UNDERCOVER OPERATION

17. Your affiant knows from training and experience that child pornography comes from many sources. Computers have revolutionized the way in which those sources and users interact. Computers have also revolutionized the way in which collectors and users of child pornography can keep their collections. The development of computers and the Internet has greatly changed and added to the way in which child pornography is disseminated, collected, and viewed.
18. Computers have facilitated the ability of child pornography collectors and traders to keep their collections hidden. Photographs and videos that were previously stored in boxes are now traded and collected as digital images that can be stored and maintained on electronic media, such as a digital storage device called a "Micro Secure Digital Card", that is smaller than a postage stamp. Computers and the Internet now aid and serve in the production of child pornography, the distribution of child pornography, the viewing of child pornography, the storage of child pornography and communication between child pornography traders.
19. One of the fast growing areas that facilitates and is used by child pornography collectors and traders is the P2P networks like FastTrack, eDonkey, Bittorrent and the Gnutella Networks. The Peer-to-peer (P2P) Networks have become ideal for traders to openly exchange collections and share those collections. The P2P network has provided a way for traders to have what they feel is an open and anonymous distribution and trading network. This network enables trading on a world-wide basis and with upload and download speeds as if the trader was next door.
20. Your affiant has personally worked undercover P2P investigations and knows from training, research, personal experience in undercover investigations involving P2P networks, and by personal participation in the undercover program the following information.
21. Your affiant knows that computers on the eDonkey and Gnutella networks have software installed on them that facilitate the trading of images. The software, when installed, allows the user to search for pictures, movies and other digital files by entering text as search terms. Some names of the software used include, but are not limited to, eDonkey, BearShare, Frostwire, LimeWire, Shareaza, Morpheus, Gnucleus, Phex and other software clients. Those are software programs that interface with the Gnutella Network and the eDonkey network.
22. P2P file sharing networks, including the Gnutella and eDonkey networks, are frequently used to

J. J. [Signature] 8/28/12
Signature: Judicial Official/Date

Additional Affiant: Signature/Date

G. [Signature] 8/28/12
Signature: Law Enforcement/Date

[Signature] 8/28/12 11
Additional Affiant: Signature/Date

trade digital files of child pornography. These files include both image and movie files.

23. P2P file sharing programs are a standard way to transfer files from one computer system to another while connected to a network, usually the Internet. Peer-to-Peer file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files.
24. Many P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.
25. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.
26. To access the P2P networks, a user first must purposely seek out P2P software for sharing on the internet and then obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide P2P network for download. Most P2P software gives each user a rating based on the number of files he/she is contributing to the network and on the user's bandwidth and firewall settings. This rating affects the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. However, a user is not required to share files to utilize the P2P network.
27. A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, information about the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results of the keyword search are displayed and the user then purposefully selects file(s) which he/she wants to download. There is no accidental download process. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Frequently, a computer forensic examiner, using these logs, can determine the Internet Protocol ("IP") address from which a particular file was obtained.
28. Thus, a person interested in sharing child pornography with others in the P2P network, need only place those files in his/her "shared" folder(s) or leave the files they download in the shared folder. Those child pornography files are then available to all users of the P2P network for download regardless of their physical location. For instance, a person interested in obtaining child pornography can open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select files from

J. Lee & Co 8/28/12
Signature: Judicial Official/Date

Additional Affiant: Signature/Date

GTBunn 8/28/12
Signature: Law Enforcement/Date

Reagan 8/28/12
Additional Affiant: Signature/Date

12

the search results and those files can be downloaded directly from the computer(s) sharing those files.

29. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time thus speeding up the rate at which a single file is downloaded. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The user's computer then reassembles those parts into the single file. This reduces the time it takes to download the file. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular Internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.
30. Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to forcefully send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her computer's active participation.
31. Based on your affiant's training and experience, your affiant also know the following about the operation of the eDonkey file-sharing network:
32. The eDonkey network is also known as the eDonkey2000 file-sharing network, or eD2k. Users of this network can simultaneously provide files to users while downloading files from other users. It is one of the many P2P networks across the globe.
33. The eDonkey network can be accessed by computers running several different client programs. These programs share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of the same client. During the default installation of an eDonkey client, settings are established which configure the host computer to share files. Depending upon the eDonkey client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.
34. Typically, a setting establishes the location of one or more directories or (shared) folders whose files are made available for distribution to other eDonkey users.
35. Typically, a setting controls whether or not other users of the network can obtain a list of the files being shared by the host computer by asking for a "browse" of the other computer's file list.
36. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.
37. Files on the eDonkey network are uniquely identified using a MD4 root hash of a MD4 hash list

J. [Signature] 8/28/12
Signature: Judicial Official/Date

G. [Signature] 8/28/12
Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

[Signature] 8/28/2012 13
Additional Affiant: Signature/Date

of pre-determined chunks of the file. This treats files with identical content but different names as the same, and files with different contents but the same name as different.

38. The ed2k hash function is a MD4 root hash of a list of MD4 hashes from the chunks of the file, and gives a different result than a simple MD4 hash: The file data is divided into full chunks of 9500 KB (9728000 bytes or nearly 9.28 MB) plus a remainder chunk, and a separate 128-bit MD4 checksum is computed for each. If the file length is an exact multiple of 9500 KB, the remainder zero size chunk is still used at the end of the hash list. The ed2k hash is computed by concatenating the MD4 checksums of all the pieces of the file in order, and hashing the resulting sum using MD4. Although, if the file is composed of a single non-full chunk, its MD4 hash is used with no further modifications. This method of hashing allows the recipient to verify that a hash list corresponds to the original ed2k file hash, without the need to have the data blocks.
39. Files located in a user's shared directory are processed by the P2P client software. As part of this processing, a MD4 root hash value is computed for each file in the user's shared directory.
40. The eDonkey network uses MD4 root hash values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses MD4 root hash values to ensure exact copies of the same file are used during this process.
41. The MD4 (or Message-Digest Algorithm) is a cryptographic hash function developed by Ronald Rives in 1990. The digest length is 128 bits. The mathematical and statistical probability of a collision is less than a collision of the same DNA in humans.
42. The eDonkey software allows the user to search for pictures, movies and other files by entering descriptive text as search terms. These terms are typically processed by peers based upon the information about the files that had been sent by individual users. Your affiant knows through personal experience the query results presented to the user of the P2P Networks allows the user to select a file from the list of files returned during a query, and then receive that file from other users around the world. Often these users can receive the selected movie from numerous sources at once. The software can balance the network load and recover
43. Entering search terms into an eDonkey client returns a list of files and descriptive information including, in some client software, the associated MD4 root hash values. Your affiant knows from training and personal experience, trial searches, and working undercover cases on the P2P networks that users can find images and movies of child pornography by using these search terms. Some examples of search terms that locate files containing child pornography are "PTHC" (which stands for "Pre-Teen Hard Core"), "babyj", "pedo", "kiddie", "underage", and various terms relating to ages such as "10yo", etc. These search terms typically results in the user being presented with a list of files that include movie and image files that when downloaded and viewed contain child pornography illegal in NC. Your affiant has tested other search terms and results and has been able to successfully identify potential child pornography on the P2P network. Your affiant knows that automated tools can be used to automate the search process for those terms and then used to identify those offering for trade, files that have those terms in them. Your affiant

J. [Signature] 8/28/12
Signature: Judicial Official/Date

[Signature] 8/28/12
Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

[Signature] 8/28/2012
Additional Affiant: Signature/Date

14

the database that evidence child pornography from previous investigations by other law enforcement officers.

55. The data acquired from automated tools and undercover operations, including hash value, IP address offering to participate in distribution of a file, name of the file, date and time it was identified by CPS provided from the suspect computer, are all compiled into a user-friendly interface. Your affiant queried CPS for a particular geographic region or jurisdiction – in this case, Rockingham County, NC. Upon selecting an IP address to investigate, the information available of the servers historically about that IP address is generated and sent by CPS for the investigating officer to review.
56. NordicMule is a software tool based on the eMule software program, a publicly available P2P client that operates on the eDonkey network. NordicMule was originally adapted from eMule by The Norway National Criminal Investigative Service for law enforcement purposes. NordicMule was then modified for law enforcement investigations to function within the CPS suite of tools, discussed above. Functionality and features were added to create a software tool that identifies computers offering to share files associated with the exploitation of children on the eDonkey network.
57. NordicMule works by regularly downloading ed2K links (eDonkey magnets) from the CPS servers. Those links are file hashes previously viewed by law enforcement and known to contain depictions of child sexual abuse. As NordicMule receives information from sharing peers about a known file, it attempts to connect and browse that peer. NordicMule identifies what each individual and specific computer is offering for transfer based on IP address. Thus the information acquired is not from multiple sources, but from specific IP addresses at specific dates and times. All information submitted to the CPS servers is the result of individual peer computers responding to a request from NordicMule. Information that is logged to the CPS servers contains the police officer's license number.
58. NordicMule searches for files of known or suspected child pornography and then records the IP addresses of those computers offering to participate in the distribution of known or suspected child pornography. NordicMule reads the publicly available information from computers that are identified as offering child sexual abuse images for distribution. This software reads these reported offers to participate in the sharing of child pornography and reports the IP address, the time, the date, the ED2K MD4 value, the type of software in use, the GUID number (or serial number) of the software, and the filename for each computer offering in a consistent and reliable manner to the undercover servers housed in Florida. Your affiant has validated this software by running identical search terms through manual methods with open source software and the automated system using NordicMule and has confirmed that NordicMule performs in the same way, with matching results as the previous manual investigative techniques used in this operation to date. The automated tools like NordicMule in use in the undercover operation provide beneficial data to undercover officers by automatically identifying and logging IP addresses that are offering to distribute child pornography. The software is distributed and run by thousands of investigators whose software then contributes to a global database. Your affiant has access to those automated logs and can check and see who in and around this jurisdiction (Rockingham County) is participating in and offering child pornography for distribution on the P2P networks.

2 2nd Jue 8/28/12
Signature: Judicial Official/Date

Signature: GT Burni Date: 8/28/12

Additional Affiant: Signature/Date


8/22/2022 17
Additional Affiant: Signature/Date

59. Your affiant then selected the option to monitor a particular IP address; in this case 24.148.156.211 on July 20, 2012. When the IP address was online in the eDonkey Network, your affiant's computer would automatically begin to download the files available for trade by the suspect computer. This is done through a law enforcement-only designed system, which your affiant refers to as Undercover Investigative Software (hereinafter referred to as UIS), currently used in state and local Peer-to-Peer P2P file sharing investigations and utilized through the CPS suite of tools. In this particular case it was used to request a download of the files of child pornography from IP address 24.148.156.211. Downloading is a transfer of data from one computer to another. Since your affiant was doing the download, your affiant was receiving data, which was transmitted from another computer. This software is designed by and for law enforcement and only available to law enforcement officers who have attended the appropriate training. Your affiant has done so and conducts that training for others. The UIS is designed to connect directly to one IP address and browse or download from one specific peer at a time using technology to block all other IP addresses from delivering any piece of the file. The UIS is a P2P file sharing client similar to other file sharing which are free and available to the public.
60. Using source code from a free P2P client, the UIS was modified by/for law enforcement to meet the stringent investigative requirements of these cases. For example, the UIS will only download files from a single source – the target IP, while the public version will download from many sources. The UIS thus takes much longer to download files because of the single source limitation. The UIS uses only publicly available P2P options which follow the programming language (protocols) set forth in the public P2P protocol standards. No functionality outside of the publicly available protocols is added, thus eliminating any potential private intrusion on the suspect IP's computer or files. The UIS uses the same code and language that is available to any and all software developers.
61. Upon locating an IP address on the P2P networks that is evidencing Hash Values of known images/videos of child pornography as acquired from the CPS, the IP address is launched into the UIS by the investigator. An automated function of the UIS will attempt to connect to the IP address when it is observed being "on-line" and send a request to browse (i.e. look at and log the information being transmitted -a file list - and/or shown by that IP) and/or download a file from the shared folder of the computer utilizing that IP address. If the connection is not made to either browse or download, the UIS automatically continues to attempt to make a connection with the IP address.
62. If a connection is made with the suspect IP address, the UIS will log the connection. It will also log the browse and/or download in the "logs" – the activity associated with that IP addresses' activity. Files are then downloaded directly into your affiant's computer and segregated from any other evidence. Prior to beginning an investigation using the UIS, your affiant creates a folder structure on the hard drive of your affiant's own computer instructing the UIS to the file path of where to store files that are downloaded and logs that are created. Both the downloaded files themselves as well as the logs will be reported in the appropriate folders created for the target peer IP address by your affiant. The logs identify that a known Hash Value of child pornography has been located, that the download transfer started, that the transfer is in fact processing, and that the transfer of the file is complete. The length of time the download process takes depends on the size of the file and speed of the internet/computer of both your affiant and the target IP's computer.


Signature: Judicial Official/Date

Additional Affiant: Signature/Date


Signature: Law Enforcement/Date


Additional Affiant: Signature/Date

63. When a file has successfully completed the download process the UIS notifies your affiant electronically. The UIS, being based on P2P program design, ensures that files are obtained directly from the target IP address – assuring a single-source download so that any downloaded file comes directly from the suspect IP address.
64. Your Affiant has validated the UIS by conducting investigations manually using publicly available P2P clients and compared the results with the automated UIS process and found the results to be exactly the same.

SPECIFIC FACTS ABOUT THE IP ADDRESS AND PLACE TO BE SEARCHED

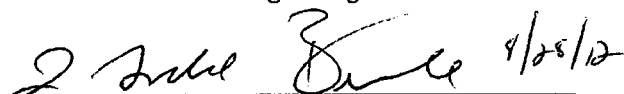
65. The IP address 24.148.156.211 was first logged in the CPS undercover system by the automated tools previously described on 07/20/2012 offering to participate in the distribution of child Pornography known to me. Between 07/20/2012 and 07/26/2012, the IP address 24.148.156.211 was logged, showing a continual pattern of child pornography, by the automated tools. That IP address was logged as offering to participate in the distribution of 3 files of known or suspected child pornography during that period of time. Of those 3 files logged your affiant has seen in prior investigation and can attest that he knows personally that 2 of them are indeed child pornography as defined by the North Carolina General Statutes. The other 1 are known by other officers participating in the undercover operation to be child pornography. The 2 that are known by your affiant can be described as follows:

Ed2k hash value: 60492779477159DD2DA1DB8EE57D6995. File name: "Ptsc Mom & Daughter In Bath.mpg." Detective Bridge has personally seen and knows the file with this digital signature to be a movie file that shows an adult female in a shower with a prepubescent female. Later in the video, the prepubescent female is show masturbating and using a vibrator. The adult female and prepubescent female engage in oral sex, along with other sex acts.

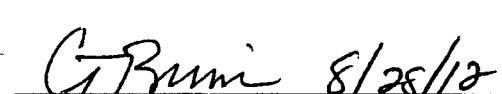
ED2k hash value: A09A2871D9140290887128F7FD593234. File Name: "(Pthc) Russia 10Yo-11Yo Little Brother And Sister-2 - Boy&Girls Fucking_ Just Posing Or Naked 1.avi". Detective Bridge has personally seen and knows the file with this digital signature to be a video that shows two preteen boys on a bed who get nude and have sex in various positions with a young teen girl. Other clips show nude children playing in the sand and in various sexual positions on a bed.

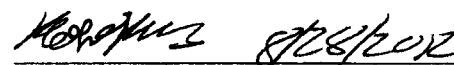
66. Utilizing the UIS, your affiant connected to the IP address 24.148.156.211 on July 21, 2012 between 0550 hrs EDT and 1639 HRS EDT and was able to directly download parts (1153339KB) of 2 video files of the sexual performance of a child. Your affiant has viewed the said file and it is believed to be Child Pornography based upon North Carolina Statutes, and is described as follows:

The file names were Mom & Daughter In Bath.mpg with an ED2k hash value of 60492779477159DD2DA1DB8EE57D6995 Detective Bridge has personally seen and knows the file with this digital signature to be a movie file that shows an adult female in a shower


Signature: Judicial Official/Date

Additional Affiant: Signature/Date


Signature: Law Enforcement/Date


Additional Affiant: Signature/Date

with a prepubescent female. Later in the video, the prepubescent female is show masturbating and using a vibrator. The adult female and prepubescent female engage in oral sex, along with other sex acts.

67. The partial downloaded version I obtained directly from IP address 24.148.156.211 matches portions of what was described above and is playable and viewable and the viewable portion contains child pornography even though it is a portion of the entire file.
68. The second file name is (Pthc) Russia 10Yo-11Yo Little Brother And Sister-2 - Boy&Girls Fucking_Just Posing Or Naked 1.avi this video shows two preteen boys on a bed who get nude and have sex in various positions with a young teen girl. Other clips show nude children playing in the sand and in various sexual positions on a bed. The partial downloaded version I obtained directly from IP address 24.148.156.211 matches portions of what was described above and is playable and viewable.
69. The UIS was also able to identify the software in use by that IP address as eMule v0.5 and also a Globally Unique Identification number associated with the computer using his IP address. The GUID associated with this address at the time of the download was 8348EFA7A30EF645C3D806F648766F26. A GUID is assigned to the computer when a file sharing program (such as E-Mule or any other peer-to-peer file sharing platform) is placed onto the computer. This series of numbers and letters is a unique serial number generated for each computer running P2P software around the world. Should the computer be used to access the Internet from a different IP address the GUID will remain the same as it is intrinsic to the computer system in almost all software programs. Further, should the user of the computer update the file sharing program with a newer version, a new GUID will be assigned to the computer for the updated program.
70. Your affiant determined, by using Internet websites that the IP address 24.148.156.211 where child pornography was downloaded from, on the dates listed above was owned by Earth Link as the Internet Service Provider (ISP). On August 7, 2012 I contacted SBI Agent Gerald Thomas who forwarded my request for an administrative subpoena to Cheryl King of the NCSBI. Ms. King filed and administrative subpoena for the IP address 24.148.156.211 for the subscriber information on July 21, 2012 at 0400 GTC. Records below indicate 24.148.156.21 was assigned to the following Earth Link customer for the time request. The following information was returned by Earth Link on August 8, 2011:

Subscriber Name: Roberta Hill
Service Address: 413 N 2nd AVE
Telephone #: 336-510-7972
User Name: ms21842365@earthlink.net

71. Time Warner's information described the IP address as issued to the above subscriber from 03/13/2009 to the date of the return of service.


[Signature] 8/18/12
Signature: Judicial Official/Date

[Signature] 8/28/12
Signature: Law Enforcement/Date

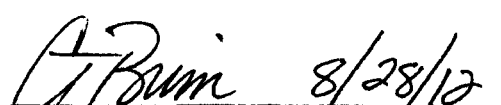
Additional Affiant: Signature/Date

[Signature] 8/28/12
Additional Affiant: Signature/Date

72. In verification of the occupants of 413 N 2nd Ave. Your affiant obtained the NC Department of Motor Vehicles Driver License information for Roberta Hill NC OL# 8867196 that information listed her current address as 413 N 2nd Ave. It listed her as having a Pontiac Sunfire registered at that address license number PWA6942. Brian David Hill is also listed with the NC Department of Motor Vehicles at this address with a NC OL# 38360908.
73. Based on the foregoing identification by IP address 24.148.156.211 a computer at the location of the IP addresses and physical address listed in this affidavit (24.148.156.211) offered for distribution files with ED2K values that are known or suspected to contain child pornography and sent to your affiant files containing child pornography. A reasonable officer with the proper training and experience could infer and conclude from the logs that the computer at the reported IP addresses recently offered for distribution files with digital signatures of known or suspected child pornography. It could also be inferred with a high degree of certainty, on your affiant's part, that the (Digital Signatures-or hash values) and IP addresses logged were sharing or offering to share those files on the eDonkey Network to other users. Therefore there is probable cause to believe that there is evidence (child pornography files and computer trace evidence listed in this warrant) of a continual pattern in July of 2012 on-going possession and distribution of child pornography through the P2P network (second degree sexual exploitation of a minor) (G.S. 14-190.17) located on the premises of 413 N 2nd Ave, Mayodan NC, the Home of Roberta Hill W/F DOB: 05/14/1967 NC OLN: 8867196 and Brian David Hill W/M DOB: 5/26/1990 NC OLN: 38360908, and/or any other person at the residence of at 413 N 2nd Ave Mayodan NC to include any vehicles located at that address: specifically registered to Roberta Hill W/F DOB: 05/14/1967 NC OLN: 8867196 that are associated with the home: a 200 Pontiac Sunfire Plate # PWA6942.
74. In your affiant's training and experience with computers your affiant has found that many individuals store their computers (laptops) inside vehicles at the residence and failure to check the vehicles may have result in not finding the computer at the residence. In your affiant's training and experience the lease of the IP address is not always the one who used the computer on the network and frequently others in homes where an IP address is assigned can just as well be the perpetrator. As a result it is imperative to search for all computers in the home and or vehicles in order to determine who actually offered child pornography and distributed child pornography to me. It is highly probable in your affiant's training and experience with this network that a household member of the account identified by Earth Link is active in possession and sharing known or suspected child pornography on the P2P network. A search of that residence where the Cable Internet subscription come back to and the computers and routers at that residence will reveal who at that residence has been involved in active participation in the distribution, possession, receipt, and sharing of child pornography files.


Signature: Judicial Official/Date

Additional Affiant: Signature/Date


Signature: Law Enforcement/Date

 21
Additional Affiant: Signature/Date

Detective Robert W. Bridge
Reidsville Police Department

Robert W. Bridge

Sworn to and subscribed before

Me this, the 28th day of August, 2012

2 Julie Anne

Judicial Official Superior Court

2 Julie Anne 8/28/12

Signature: Judicial Official/Date

CT Bruni 8/28/12

Signature: Law Enforcement/Date

Additional Affiant: Signature/Date

Robert W. Bridge 8/28/2012

Additional Affiant: Signature/Date

22